UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,251	03/30/2004	Satyajit Nath	2222.5500000	8159

26111 7590 06/22/2010

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
06/22/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/815,251	NATH, SATYAJIT	
	Examiner	Art Unit	
	JUNG KIM	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 April 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) *13-28 and 46* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12 and 29-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's election of claims filed on 4/1/10.

2. Claims 1-46 are pending.

3. Applicant elects claims 1-12 and 29-45.

Restriction Requirement

4. In the Reply to the Restriction Requirement, Applicant elected claims 1-12 and 29-45. It is noted that Applicant's remarks in the reply is unclear. Applicant states that the election is made without traverse ("This election is made without traverse"), but then requests reconsideration and withdrawal of the restriction requirement ("Reconsideration and withdrawal of the Restriction Requirement, and consideration and allowance of all pending claims, are respectfully requested"). Applicant's contention appears to be that the grouping of claims 13-28 and 46 is improper because these claims are not directed to the same scope of invention. Claims 13-19 and 46, and claims 20-28 do recite material differences (claims 20-28 recite that the electronic document includes a header portion that includes key data whereas claims 13-19 and 46 do not recite such limitations); however, these differences do not pose an undue burden on the examination. Hence, the original grouping of inventions I and II (claims 1-12 and 29-45, and claims 13-28 and 46) is maintained.

Response to Arguments

5. Applicant's arguments against the 102 rejection of claim 1 have been considered but are not persuasive. On pgs. 16-19 of the Remarks, applicant alleges that Merriam does not anticipate claim 1 because the prior art does not teach the limitation "cryptographically associating, using a cryptographic key, the document retention policy with the electronic document." The following portion of Applicant's specification (pg. 11, paragraph 47) is pertinent to ascertain the scope of this limitation:

> Next, the document retention policy is cryptographically imposed 206 on the electronic document. Recall, however, that the document retention policy at this point is based on a future event which is presently unscheduled. In one implementation, a cryptographic key is utilized to encrypt the electronic document so that access to the electronic document can be restricted after the document retention policy has been exceeded. In other words, after the period of time for document retention specified by the document retention policy has been exceeded, the cryptographic key that is needed to gain access to the electronic document is no longer made available to users. As a result, because the electronic document was previously cryptographically secured using a cryptographic key, if the corresponding or counterpart cryptographic key is no longer available, then the electronic document remains encrypted and thus unusable. In any case, following the operation 206, the retention policy assignment process 200 is complete and ends.

6. In view of is portion of the specification, the limitation "cryptographically associating, using a cryptographic key, the document retention policy with the electronic document" is anticipated by any invention where a cryptographic key is used to encrypt an electronic document and access to the cryptographic key depends on a retention policy. This is exactly what Merriam discloses. In Merriam, a retention manager uses an encryption key to encrypt an information set, and then stores the encryption key in a key repository and the encrypted information set in an information repository. When the retention policy implemented by the manager indicates that the stored encrypted

information set should be purged, the stored encryption key is deleted, thereby preventing a client from gaining access to the contents of the encrypted information set. See Merriam, col. 4, line 60-col. 6, line 44. Therefore, Applicant's arguments are not persuasive and claim 1 remains rejected as being anticipated by Merriam.

Allowable Subject Matter

7. The indicated allowability of claims 13-37 and allowable subject matter of claim 2-12 are withdrawn after further consideration of the teachings of Merriam and Todd. The rejections follow.

Claim Rejections - 35 USC § 101

8. Claims 29, 30, 32-44 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 29, 30 and 32 define a method for distributing cryptographic keys used in a file security system. However, none of these steps require machine implementation; these steps are merely abstract procedures for denying access to a document retention key if a document retention period has been exceeded. Hence, the method is not tied to a particular machine. Furthermore there is no transformation of an article or representation of an article (the method only discloses refusing to distribute the document retention key) See In re Bilski, 2007-1130 at 15, ("At present, however, and certainly for the present case, we see no need for such a departure and reaffirm that the machine-or-transformation test, properly applied, is the governing test for determining patent eligibility of a process

under § 101." The Court also points to the Abele case where a dependent process claim was determined to be statutory under 101 but not the independent claim; the dependent claim was a sufficiently specific transformation because it changed "raw data into a particular visual depiction of a physical object on a display"; the transformed object must be "physical objects or substances" or "representative of physical objects or substances," id. at 30 and 32).

9. Claims 33-37 are directed to a security system comprising a "key store" and "an access manager." Under the broadest reasonable interpretation of the claims, a key store and access manger are programs per se. See specification, pg. 25, paragraph 96 (the invention can be implemented by software). Programs are not one of the four statutory categories of patent eligible subject matter. See In re Nuijten.

10. Claims 38-44 now recite a "tangible computer readable medium." However, this language still broad enough to include signal claims-signals is physical and hence tangible. In view of Applicant's specification (see pg. 25, paragraph 96), a tangible computer readable medium is directed to propagating signals, which are not one of the four statutory categories of patent eligible subject matter.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

12. Claims 38-44 are rejected under 35 U.S.C. 102(a) as being anticipated by a conventional Compact Disc storing text data.

13. Claims 38-44 define a computer readable medium having instructions stored thereon for providing data retention for electronic data. However, mere instructions stored on a computer readable medium is nonfunctional printed matter, and non functional printed matter cannot be used to distinguish over a CD storing text data because there is no functional relationship between the instructions and the computer readable medium.

14. Claims 1-3 and 33-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Merriam US 6,915,435 (hereinafter Merriam).

15. As per claims 1-3, Merriam discloses a method of electronic document retention, comprising:

a. assigning a document retention policy to the electronic document, the document retention policy being based on a future event that is unscheduled (col. 4:21-49, retention manager manages the retention of "information sets" based on

a time period, condition policy, classification-based policy or any combinations there of);

b. cryptographically associating, using a cryptographic key, the document retention policy with the electronic document (4:12-31, document is encrypted using a public key, the corresponding private key is stored in a key repository, and key availability is dependent on the retention policy for the encrypted information set);

c. determining whether the future event has occurred; and cryptographically preventing access to the electronic document in accordance with the document retention policy based on the occurrence of the future event (4:60-6:44, when a condition is met, the decryption key is deleted by the retention manager, thereby preventing decryption of the encrypted information set);

d. the determining is performed periodically (fig. 3, retention policy is checked cyclically; periodic checking is de facto standard).

16. As per claims 33-37, Merriam discloses a file security system for restricting access to electronic files, said file security system comprising:

e. a key store that stores a plurality of cryptographic key pairs, each of the cryptographic key pairs including a public key and a private key, at least one of the cryptographic key pairs pertaining to a retention policy (fig. 1, reference no. 114 "key repository", col. 4:12-20, public/private keys; public keys are used to

encrypt the information sets), the retention policy being dependent on a future event (4:36-49, retention policies are based on conditions); and

f. an access manager operatively connected to said key store, said access manager determines whether the private key of the at least one of the cryptographic key pairs pertaining to the retention policy is permitted to be provided to a requestor based on whether the future event has occurred, wherein the requestor requires the private key of the at least one of the cryptographic key pairs pertaining to the retention policy to access a secured electronic file, and wherein the secured electronic file was previously secured using the public key of the at least one of the cryptographic key pairs pertaining to the retention policy, and at the time the electronic file was so secured, the future event was unscheduled (fig. 1, reference no. 116 "retention manager"; 4:28-49, retention manager manages the retention of "information sets" based on a time period, condition policy, classification-based policy or any combinations there of; 5:11-55, encrypting the received information set with a cryptographic key);

g. wherein said access manager prevents the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time from being provided to the requestor after a predetermined retention period following the occurrence of the future event (5:56-6:13, 6:27-44, the decryption key is deleted if the encrypted information set is to be purged based on the retention policy);

h. wherein the requestor is a client module that operatively connects to said access manager over a network (fig. 1, reference no. 106, "information sink", 3:32-49);

i. wherein said file security system further comprises: at least one client module, configured assist in selecting the retention policy and secure the electronic file using the public key of the at least one of the cryptographic key pairs pertaining to the retention policy so as to cryptographically impose the retention policy (4:33-49, 6:14-26, retention manager operates by implementing a predetermined information retention policy; see generally, figure 6 and col. 8:39-44);

j. wherein said file security system further comprises: at least one client module, said client module assisting with unsecuring the secured electronic file by acquiring the private key of the at least one of the cryptographic key pairs that pertains to the retention policy from said key store if permitted by said access manager, and then unsecuring the secured electronic file using the private key of the at least one of the cryptographic key pairs that pertains to the retention policy (7:20-8:7, information sink acquires decryption key from the information manager).

17. As per claims 38-41, Merriam discloses a tangible computer readable medium for having instructions stored thereon for providing data retention for electronic data, the instructions comprising:

k. instructions to assign computer program code for assigning a data retention policy to the electronic data, the data retention policy being based on a future event that is unscheduled (col. 4:21-49, retention manager manages the retention of "information sets" based on a time period, condition policy, classification-based policy or any combinations there of);

l. instructions to cryptographically associate, using a cryptographic key, computer program code for cryptographically associating the data retention policy with the electronic data (4:12-31, document is encrypted using a public key, the corresponding private key is stored in a key repository, and key availability is dependent on the retention policy for the encrypted information set);

m. wherein said computer readable medium the instructions further comprise: instructions to cryptographically prevent computer program code for cryptographically preventing access to the electronic data in accordance with the data retention policy based on the occurrence of the future event (4:21-49, 6:27-44, decryption keys are deleted when corresponding information set is to be purged under the retention policy);

n. wherein the electronic data is an electronic file; wherein the electronic data is an electronic document (3:20-31, information set broadly refers to any digital data including files).

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 4-8 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merriam.

20. As per claims 4-8 and 45, the rejection under 35 USC 102(e) as being anticipated by Merriam is incorporated herein. Furthermore, Merriam discloses the retention manager implements a retention policy, whereby the manager determines if a stored information set should be retained based on a condition. Although Merriam does not disclose a network accessible resource whereby the resource determines if a condition has occurred based on a future event description transmitted over the Internet, it is notoriously well known in the art to distribute process handling to remote systems. This concept is known as distributive processing. Distributive processing utilizes a collection of computers that communicate over a network to perform different processing roles within a larger framework. One means by which remote computers perform such tasks is the use of remote procedure calls (RPC). Distributive processing enables the workload to be segregated based on a separation of concerns. Official notice of this teaching is taken. It would be obvious to one of ordinary skill in the art at the time the invention was made wherein the determining comprises interacting with a

network accessible resource; wherein the determining comprises interacting with a web accessible resource; the determining comprises: supplying a future event description of the future event to the web accessible resource; and determining, at the web accessible resource, whether the future event has occurred; wherein said supplying is achieved by a universal resource locator associated with the future event description; and wherein the determining comprises: supplying the future event description to a contract management system; determining, at the contract management system, whether the future event has occurred; and supplying a future event description of the future event to the network accessible resource; and determining, at the network accessible resource, whether the future event has occurred. One would be motivated to do so to enable the workload to be segregated based on a separation of concerns. The aforementioned cover the limitations of claims 4-8 and 45.

21. Claims 9-12, 29-32 and 42-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merriam in view of Todd et al. US 7,249,251 (hereinafter Todd).

22. As per claims 9-12, the rejection of claim 1 under 35 USC 102(e) as being anticipated by Merriam is incorporated herein. In addition, Merriam discloses deactivating the cryptographic key in response to determining that a document retention period has expired, thereby preventing further access to the electronic document. See Merriam, col. 4:21-49, 6:27-44 (decryption keys are deleted when corresponding information set is to be purged under the retention policy; retention policies can be

based on retention periods). Furthermore, as noted above, on col. 4:21-49, Merriam discloses that the retention manager manages the retention of "information sets" based on a time period, condition policy, classification-based policy or any combinations there of. However, Merriam does not expressly disclose the document retention policy specifies a document retention period based on the future event; wherein the document retention policy specifies a document retention period that expires a predetermined period of time after the occurrence of the future event; and permitting the deactivating step to be overridden so that the electronic document can remain accessible even after the document retention period. Todd discloses a method and apparatus for secure modification of a retention period for data in a storage system, where data is retained for a specified period after a future event. See col. 6:53-61 (x-rays are retained 2 years after the death of patient). Modifications can be made to either shorten or extend the original retention period. See col. 7:7-50. It would be obvious to one of ordinary skill in the art at the time the invention was made for the document retention policy specifies a document retention period based on the future event; wherein the document retention policy specifies a document retention period that expires a predetermined period of time after the occurrence of the future event; and permitting the deactivating step to be overridden so that the electronic document can remain accessible even after the document retention period. One would be motivated to do so to enable retention period modification as taught by Todd. The aforementioned cover the limitations of claims 9-12.

23. As per claims 29-32, Merriam discloses a method for distributing cryptographic keys used in a file security system, said method comprising:

o. receiving a request for a document retention key that is necessary to gain access to a cryptographically secured electronic document (7:20-8:7, information sink acquires decryption key from the information manager);

p. identifying a document retention period associated with the document retention key; determining whether the document retention period associated with the document retention key has been exceeded; and refusing to distribute the document retention key in response to determining that the document retention period for the electronic document has been exceeded (col. 4:21-49, 6:27-44, decryption keys are deleted when corresponding information set is to be purged under the retention policy; col. 4:21-49, the retention manager manages the retention of "information sets" based on a time period, condition policy, classification-based policy or any combinations there of);

q. wherein said method is performed at a server, and wherein the request for the document retention key is from a client module that is connectable to the server via a network (3:32-48, information system can be a server and information sink would be a client).

24. Merriam does not disclose the document retention period being dependent on a future event that was unscheduled when the document retention period was associated with the electronic document; wherein the document retention period is a predetermined period of time after the occurrence of the future event; and wherein the document

retention period can be extended to permit extended access to the electronic document. Todd discloses a method and apparatus for secure modification of a retention period for data in a storage system, where data is retained for a specified period after a future event. See col. 6:53-61 (x-rays are retained 2 years after the death of patient). Modifications can be made to either shorten or extend the original retention period. See col. 7:7-50. It would be obvious to one of ordinary skill in the art at the time the invention was made for the document retention period to be dependent on a future event that was unscheduled when the document retention period was associated with the electronic document; wherein the document retention period is a predetermined period of time after the occurrence of the future event; and wherein the document retention period can be extended to permit extended access to the electronic document. One would be motivated to do so to enable retention period modification as taught by Todd. The aforementioned cover the limitations of claims 29-32.

25. As per claims 42-44, the rejection of claim 38 under 35 USC 102(e) as being anticipated by Merriam is incorporated herein. In addition, Merriam discloses instructions to deactivate computer program code for deactivating the cryptographic key in response to determining that the data retention period has expired, thereby preventing further access to the electronic data; and the instructions further comprises: instructions to determine computer program code for determining whether the data retention period has expired. See Merriam col. 4:21-49, 6:27-44 (decryption keys are deleted when corresponding information set is to be purged under the retention policy).

Furthermore, as noted above, on col. 4:21-49, Merriam discloses that the retention manager manages the retention of "information sets" based on a time period, condition policy, classification-based policy or any combinations there of. However, Merriam does not expressly disclose the data retention policy specifies a data retention period based on the future event; wherein: the data retention policy specifies a data retention period that expires a predetermined period of time after the occurrence of the future event; and wherein the instructions further comprises: instructions to permit deactivation of the cryptographic key computer program code for permitting said computer program code for deactivating to be overridden so that the electronic data can remain accessible even after the data retention period. Todd discloses a method and apparatus for secure modification of a retention period for data in a storage system, where data is retained for a specified period after a future event. See col. 6:53-61 (x-rays are retained 2 years after the death of patient). Modifications can be made to either shorten or extend the original retention period. See col. 7:7-50. It would be obvious to one of ordinary skill in the art at the time the invention was made for the data retention policy to specify a data retention period based on the future event; wherein: the data retention policy specify a data retention period that expires a predetermined period of time after the occurrence of the future event; and wherein the instructions further comprises: instructions to permit deactivation of the cryptographic key computer program code for permitting said computer program code for deactivating to be overridden so that the electronic data can remain accessible even after the data retention period. One would be motivated to do

so to enable retention period modification as taught by Todd. The aforementioned cover the limitations of claims 42-44.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2432